

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-163235

(43)Date of publication of application : 07.06.2002

(51)Int.Cl.

G06F 15/00

(21)Application number : 2000-361571

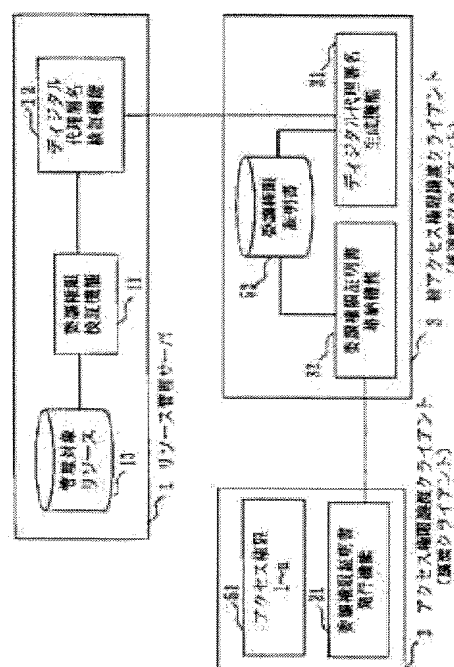
(71)Applicant : MITSUBISHI ELECTRIC CORP

(22)Date of filing : 28.11.2000

(72)Inventor : NAKANO HATSUMI  
NAKAKAWAJI TETSUO**(54) ACCESS AUTHORIZATION TRANSFER DEVICE, SHARED RESOURCE MANAGEMENT SYSTEM AND ACCESS AUTHORIZATION SETTING METHOD****(57)Abstract:**

**PROBLEM TO BE SOLVED:** To easily realize assignment of a temporary access authorization and assignment of a specified type of access authorization to a device without access authorization to a shared resource.

**SOLUTION:** A transfer client 2 issues an assignment authorization certificate 52 certifying temporary or definite transfer of access authorization to a management subject resource 13 by using an assignment authorization certificate issuing function 21, a transferred client 3 obtains the assignment authorization certificate 52 through an assignment authorization certificate storing function 32, and generates a digital agent signature which is an access request according to the obtained assignment authorization certificate 52 by a digital agent signature generating function 31. A resource management server 1 receives the digital agent signature, and verifies whether an access to the management subject resource by the transferred client 3 is properly requested or not through the digital agent signature verifying function 12 and an assignment authorization verifying function 11.





(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号  
特開2002-163235  
(P2002-163235A)

(43)公開日 平成14年6月7日(2002.6.7)

(51)Int.Cl.<sup>7</sup>

G 0 6 F 15/00

識別記号

3 3 0

F I

G 0 6 F 15/00

テーマコード\*(参考)

3 3 0 D 5 B 0 8 5

審査請求 未請求 請求項の数16 O L (全 12 頁)

(21)出願番号 特願2000-361571(P2000-361571)

(22)出願日 平成12年11月28日(2000.11.28)

(71)出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72)発明者 中野 初美

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(72)発明者 中川路 哲男

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(74)代理人 100099461

弁理士 溝井 章司 (外2名)

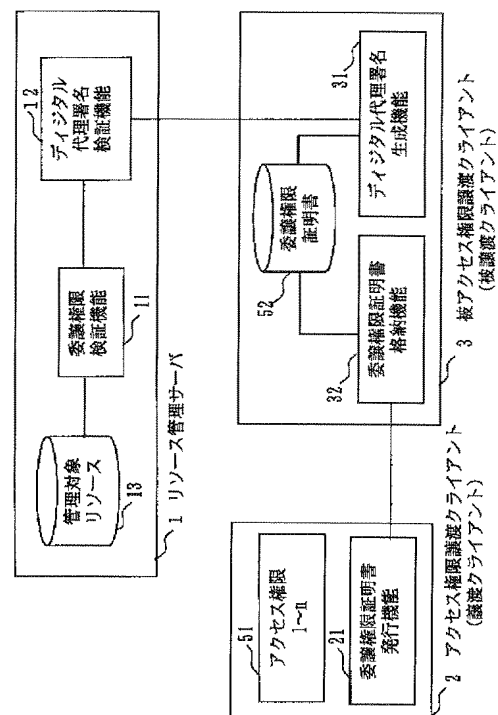
Fターム(参考) 5B085 AE06 BC07

(54)【発明の名称】 アクセス権限譲渡装置、共有リソース管理システム及びアクセス権限設定方法

(57)【要約】

【課題】 共有リソースへのアクセス権限を持たない装置に対して、一時的なアクセス権限の委譲及び特定種類のアクセス権限の委譲を容易に実現する。

【解決手段】 譲渡クライアント2が、委譲権限証明書発行機能21を用いて管理対象リソース13に対するアクセス権限の一時的又は限定的な譲渡を証明する委譲権限証明書52を発行し、被譲渡クライアント3は、委譲権限証明書格納機能32を通じて委譲権限証明書52を取得し、取得した委譲権限証明書52に基づくアクセス要求であるデジタル代理署名をデジタル代理署名生成機能31により生成し、リソース管理サーバ1はデジタル代理署名を受け取り、デジタル代理署名検証機能12及び委譲権限検証機能11を通じて、被譲渡クライアント3による管理対象リソースへのアクセスが要求適正であるか否かの検証を行う。



## 【特許請求の範囲】

【請求項1】 共有リソースへのアクセス権限を所有し、前記アクセス権限を有しない無権限装置に対して、自己の所有する前記アクセス権限の少なくとも一部を譲渡することを特徴とするアクセス権限譲渡装置。

【請求項2】 前記アクセス権限譲渡装置は、前記無権限装置が前記共有リソースにアクセスできるアクセス有効期間を限定して前記無権限装置に対して前記アクセス権限を譲渡することを特徴とする請求項1に記載のアクセス権限譲渡装置。

【請求項3】 前記アクセス権限譲渡装置は、前記共有リソースへの複数種のアクセス権限を所有し、前記複数種のアクセス権限のうち特定種類のアクセス権限に限定して前記無権限装置に対して前記アクセス権限を譲渡することを特徴とする請求項1に記載のアクセス権限譲渡装置。

【請求項4】 前記アクセス権限譲渡装置は、前記無権限装置に対する前記アクセス権限の少なくとも一部の譲渡を証明するアクセス権限譲渡証明を発行するアクセス権限譲渡証明発行部を有することを特徴とする請求項1に記載のアクセス権限譲渡装置。

【請求項5】 前記アクセス権限譲渡装置は、更に、前記無権限装置より、前記アクセス権限譲渡証明の発行を要求するアクセス権限譲渡証明発行要求を受け付けるアクセス権限譲渡証明発行要求受付部を有し、前記アクセス権限譲渡証明発行部は、前記アクセス権限譲渡証明発行要求受付部により受け付けられた前記アクセス権限譲渡証明発行要求に対して前記アクセス権限譲渡証明を発行することを特徴とする請求項4に記載のアクセス権限譲渡装置。

【請求項6】 共有リソースを管理する共有リソース管理装置と、前記共有リソースへのアクセス権限を所有するアクセス権限所有装置と、前記アクセス権限を有しない無権限装置とを有する共有リソース管理システムであって、前記アクセス権限所有装置は、前記無権限装置に対して、自己の所有する前記アクセス権限の少なくとも一部を譲渡し、前記無権限装置は、前記アクセス権限所有装置より譲渡された前記アクセス権限に従って前記共有リソースにアクセスし、前記共有リソース管理装置は、前記無権限装置による前記共有リソースへのアクセスが、前記アクセス権限所有装置により譲渡された前記アクセス権限に従った適正アクセスであるか否かを検証することを特徴とする共有リソース管理システム。

【請求項7】 前記アクセス権限所有装置は、前記無権限装置に対して、前記無権限装置が前記共有リソースにアクセスできるアクセス有効期間を限定して前記アクセス権限を譲渡し、

前記無権限装置は、前記アクセス権限所有装置より譲渡された前記アクセス権限に従って前記共有リソースにアクセスし、

前記共有リソース管理装置は、前記無権限装置による前記共有リソースへのアクセスが、前記アクセス権限の前記アクセス有効期間の限定に従った適正アクセスであるか否かを検証することを特徴とする請求項6に記載の共有リソース管理システム。

【請求項8】 前記アクセス権限譲渡装置は、前記共有リソースへの複数種のアクセス権限を所有し、前記複数種のアクセス権限のうち特定種類のアクセス権限に限定して前記無権限装置に対して前記アクセス権限を譲渡し、

前記無権限装置は、前記アクセス権限所有装置より譲渡された前記アクセス権限に従って前記共有リソースにアクセスし、

前記共有リソース管理装置は、前記無権限装置による前記共有リソースへのアクセスが、前記特定種類のアクセス権限への限定に従った適正アクセスであるか否かを検証することを特徴とする請求項6に記載の共有リソース管理システム。

【請求項9】 前記アクセス権限所有装置は、前記無権限装置に対する前記アクセス権限の少なくとも一部の譲渡を証明するアクセス権限譲渡証明を発行するアクセス権限譲渡証明発行部を有し、

前記無権限装置は、前記アクセス権限所有装置により発行された前記アクセス権限譲渡証明を取得し、取得した前記アクセス権限譲渡証明と前記共有リソースへのアクセス要求内容とを含むアクセス要求を生成するアクセス要求生成部を有し、前記共有リソース管理装置は、前記無権限装置により生成された前記アクセス要求を取得し、前記アクセス要求に含まれる前記アクセス要求内容が前記アクセス要求に含まれるアクセス権限譲渡証明に従った適正アクセスであるか否かを検証するアクセス要求検証部を有することを特徴とする請求項6に記載の共有リソース管理システム。

【請求項10】 前記共有リソース管理システムは、更に、

前記共有リソース管理装置より、前記アクセス要求に含まれる前記アクセス要求内容と前記共有リソース管理装置により検証された前記アクセス要求内容の適正性の検証結果を取得し、取得した前記アクセス要求内容と前記検証結果を記録する監査ログ記録装置を有することを特徴とする請求項9に記載の共有リソース管理システム。

【請求項11】 前記共有リソース管理システムは、更に、前記アクセス権限所有装置より前記アクセス権限譲渡証明を取得し、取得した前記アクセス権限譲渡証明の適正性を判断し、適正と判断されたアクセス権限譲渡証明を

前記無権限装置に配布するアクセス権限譲渡証明認証装置を有することを特徴とする請求項 10 に記載の共有リソース管理システム。

【請求項 12】 前記共有リソース管理装置は、前記アクセス権限所有装置より前記アクセス権限譲渡証明を取得し、取得した前記アクセス権限譲渡証明の適正性を判断し、適正と判断されたアクセス権限譲渡証明を前記無権限装置に配布することを特徴とする請求項 10 に記載の共有リソース管理システム。

【請求項 13】 共有リソースへのアクセス権限を有しない無権限装置に対して、前記アクセス権限の少なくとも一部を設定することを特徴とするアクセス権限設定方法。

【請求項 14】 前記アクセス権限設定方法は、前記無権限装置が前記共有リソースにアクセスできるアクセス有効期間を限定して前記無権限装置に対して前記アクセス権限を設定することを特徴とする請求項 13 に記載のアクセス権限設定方法。

【請求項 15】 前記共有リソースへの前記アクセス権限は複数種あり、複数種のアクセス権限のうち特定種類のアクセス権限に限定して前記無権限装置に対して前記アクセス権限を設定することを特徴とする請求項 13 に記載のアクセス権限設定方法。

【請求項 16】 前記アクセス権限設定方法は、前記無権限装置に対する前記アクセス権限の少なくとも一部の設定を証明するアクセス権限設定証明を発行するアクセス権限設定証明発行ステップを有することを特徴とする請求項 13 に記載のアクセス権限設定方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、システムリソースへのアクセス制御をセキュアに行う制御方式に関するものである。

【0002】

【従来の技術】 ワークステーションやパーソナルコンピュータがネットワークに接続され、ハードウェアやソフトウェア、データ等のリソースを相互に共有するような分散ネットワーク環境において、従来よりリソースへの代理アクセス方式が提案されている。たとえば、図 13 は従来のリソースへのアクセス方式である。本来のアクセス権をもつノード A 700 には

- ・ 代理アクセスを要求する代理要求部 720
- ・ ノード A のみが保持する秘密情報を管理する秘密情報管理部 710 がある。

アクセス権を委譲されるノード B 800 には

- ・ ノード A からの代理要求を処理する代理要求受付部 810
- ・ ノード A からの代理要求中にある秘密情報を保持する秘密情報管理部 820

- ・ ノード B のみが保持する秘密情報を管理する秘密情報管理部 840

- ・ ノード A の代わりにリソースにアクセスするための代理実行部 830

- ・ ユーザ処理要求の結果を提示する出力手段がある。

アクセスされるリソースを保持するノード N900 には

- ・ ノード A の秘密情報を管理する秘密情報管理部 910 がある。

【0003】 次に動作について説明する。

【0004】 ノード A がノード N にアクセスする場合、次の手順で行われる。

(1) ノード A の代理要求部 720 が秘密情報管理部 710 で管理されている秘密情報と自ノードの識別子 A を含む代理要求メッセージを生成し、ノード B に送付する。

(2) ノード B の代理要求受付部 810 はノード A からの代理要求メッセージを受信し、当該メッセージ中の秘密情報を秘密情報管理部 820 に格納する。

(3) 代理実行部 830 では、秘密情報管理部 820 よりノード A の秘密情報を取得し、ノード N900 に対する認証用メッセージを生成してノード N900 に送付する。

(4) ノード N900 は、ノード A 700 の秘密情報を用いて、認証用メッセージの検証を実施する。

(5) 検証に成功すると、ノード B がノード N のリソースにアクセス可能となる。

【0005】

【発明が解決しようとする課題】 従来の技術では、リソースへのアクセス権限の譲渡は、譲渡者、被譲渡者、リソース管理者のユーザ認証によって実現されていたため、譲渡する際は全アクセス権を譲渡する。このため、譲渡者の持つ全アクセス権のうち、任意のアクセス権を譲渡することができなかった。また、期限を過ぎた場合のアクセス権限委譲の廃止を実現するには、ユーザ側が期限内か否かを意識しなければならず、ユーザ負担が大きいという問題があった。

【0006】 この発明は上記のような問題点を解決するためになされたもので、リソースへの一時的なアクセス権限委譲及び特定種類のアクセス権限委譲を容易に実現することを目的とする。

【0007】

【課題を解決するための手段】 この発明に係るアクセス権限譲渡装置は、共有リソースへのアクセス権限を所有し、前記アクセス権限を有しない無権限装置に対して、自己の所有する前記アクセス権限の少なくとも一部を譲渡することを特徴とする。

【0008】 前記アクセス権限譲渡装置は、前記無権限装置が前記共有リソースにアクセスできるアクセス有効期間を限定して前記無権限装置に対して前記アクセス権限を譲渡することを特徴とする。

【0009】前記アクセス権限譲渡装置は、前記共有リソースへの複数種のアクセス権限を所有し、前記複数種のアクセス権限のうち特定種類のアクセス権限に限定して前記無権限装置に対して前記アクセス権限を譲渡することを特徴とする。

【0010】前記アクセス権限譲渡装置は、前記無権限装置に対する前記アクセス権限の少なくとも一部の譲渡を証明するアクセス権限譲渡証明を発行するアクセス権限譲渡証明発行部を有することを特徴とする。

【0011】前記アクセス権限譲渡装置は、更に、前記無権限装置より、前記アクセス権限譲渡証明の発行を要求するアクセス権限譲渡証明発行要求を受け付けるアクセス権限譲渡証明発行要求受付部を有し、前記アクセス権限譲渡証明発行部は、前記アクセス権限譲渡証明発行要求受付部により受け付けられた前記アクセス権限譲渡証明発行要求に対して前記アクセス権限譲渡証明を発行することを特徴とする。

【0012】この発明に係る共有リソース管理システムは、共有リソースを管理する共有リソース管理装置と、前記共有リソースへのアクセス権限を所有するアクセス権限所有装置と、前記アクセス権限を有しない無権限装置とを有する共有リソース管理システムであって、前記アクセス権限所有装置は、前記無権限装置に対して、自己の所有する前記アクセス権限の少なくとも一部を譲渡し、前記無権限装置は、前記アクセス権限所有装置より譲渡された前記アクセス権限に従って前記共有リソースにアクセスし、前記共有リソース管理装置は、前記無権限装置による前記共有リソースへのアクセスが、前記アクセス権限所有装置により譲渡された前記アクセス権限に従った適正アクセスであるか否かを検証することを特徴とする。

【0013】前記アクセス権限所有装置は、前記無権限装置に対して、前記無権限装置が前記共有リソースにアクセスできるアクセス有効期間を限定して前記アクセス権限を譲渡し、前記無権限装置は、前記アクセス権限所有装置より譲渡された前記アクセス権限に従って前記共有リソースにアクセスし、前記共有リソース管理装置は、前記無権限装置による前記共有リソースへのアクセスが、前記アクセス権限の前記アクセス有効期間の限定に従った適正アクセスであるか否かを検証することを特徴とする。

【0014】前記アクセス権限譲渡装置は、前記共有リソースへの複数種のアクセス権限を所有し、前記複数種のアクセス権限のうち特定種類のアクセス権限に限定して前記無権限装置に対して前記アクセス権限を譲渡し、前記無権限装置は、前記アクセス権限所有装置より譲渡された前記アクセス権限に従って前記共有リソースにアクセスし、前記共有リソース管理装置は、前記無権限装置による前記共有リソースへのアクセスが、前記特定種類のアクセス権限への限定に従った適正アクセスである

か否かを検証することを特徴とする。

【0015】前記アクセス権限所有装置は、前記無権限装置に対する前記アクセス権限の少なくとも一部の譲渡を証明するアクセス権限譲渡証明を発行するアクセス権限譲渡証明発行部を有し、前記無権限装置は、前記アクセス権限所有装置により発行された前記アクセス権限譲渡証明を取得し、取得した前記アクセス権限譲渡証明と前記共有リソースへのアクセス要求内容とを含むアクセス要求を生成するアクセス要求生成部を有し、前記共有リソース管理装置は、前記無権限装置により生成された前記アクセス要求を取得し、前記アクセス要求に含まれる前記アクセス要求内容が前記アクセス要求に含まれるアクセス権限譲渡証明に従った適正アクセスであるか否かを検証するアクセス要求検証部を有することを特徴とする。

【0016】前記共有リソース管理システムは、更に、前記共有リソース管理装置より、前記アクセス要求に含まれる前記アクセス要求内容と前記共有リソース管理装置により検証された前記アクセス要求内容の適正性の検証結果を取得し、取得した前記アクセス要求内容と前記検証結果を記録する監査ログ記録装置を有することを特徴とする。

【0017】前記共有リソース管理システムは、更に、前記アクセス権限所有装置より前記アクセス権限譲渡証明を取得し、取得した前記アクセス権限譲渡証明の適正性を判断し、適正と判断されたアクセス権限譲渡証明を前記無権限装置に配布するアクセス権限譲渡証明認証装置を有することを特徴とする。

【0018】前記共有リソース管理装置は、前記アクセス権限所有装置より前記アクセス権限譲渡証明を取得し、取得した前記アクセス権限譲渡証明の適正性を判断し、適正と判断されたアクセス権限譲渡証明を前記無権限装置に配布することを特徴とする。

【0019】この発明に係るアクセス権限設定方法は、共有リソースへのアクセス権限を有しない無権限装置に対して、前記アクセス権限の少なくとも一部を設定することを特徴とする。

【0020】前記アクセス権限設定方法は、前記無権限装置が前記共有リソースにアクセスできるアクセス有効期間を限定して前記無権限装置に対して前記アクセス権限を設定することを特徴とする。

【0021】前記共有リソースへの前記アクセス権限は複数種あり、複数種のアクセス権限のうち特定種類のアクセス権限に限定して前記無権限装置に対して前記アクセス権限を設定することを特徴とする。

【0022】前記アクセス権限設定方法は、前記無権限装置に対する前記アクセス権限の少なくとも一部の設定を証明するアクセス権限設定証明を発行するアクセス権限設定証明発行ステップを有することを特徴とする。

【0023】

【発明の実施の形態】実施の形態1. 図1は本発明に係る共有リソース管理システムのブロック構成図である。図において、1は管理対象リソース（共有リソース）13を管理するリソース管理サーバ（共有リソース管理装置）、2は管理対象リソース13へのアクセス権限を持つ譲渡クライアント（アクセス権限譲渡装置、アクセス権限所有装置）、3は管理対象リソース13へのアクセス権限を譲渡クライアント2から譲渡される被譲渡クライアント（無権限装置）である。

【0024】次に譲渡クライアント2から被譲渡クライアント3に、管理対象リソース13へのアクセス権限を委譲する際の動作について説明する。譲渡クライアント2は管理対象リソース13に対して、n個のアクセス種類（51-1、51-2、…、51-n）から構成されているアクセス権限51を持つ。譲渡クライアント2が被譲渡クライアント3にアクセス種類j、kを委譲する場合は、大きく2つの処理に分けられる。委譲権限証明書52の発行と、委譲権限証明書52を使って被譲渡クライアント3がリソースアクセスする処理である。

【0025】ここで、委譲権限証明書52（アクセス権限譲渡証明）とは、譲渡クライアント2が被譲渡クライアント3に対してアクセス権限を譲渡したことを証明するデータであり、委譲権限証明書52の例を図2に示す。委譲権限証明書中には、譲渡クライアント、被譲渡クライアント、委譲されるアクセス権限（例ではj、k）、委譲有効期限を委譲内容として含み、また委譲内容に対する譲渡者による署名もあわせて記載される。署名は、PKCS（Public-Key-Cryptography-Standard）#7に基づいた形式とする。

【0026】次に、譲渡クライアント2による委譲権限証明書発行の処理ステップを以下にて説明する。

【0027】（Step 1-1）譲渡クライアント2は委譲権限証明書発行機能（アクセス権限譲渡証明発行部）21により、被譲渡クライアント3に対して委譲権限証明書52を発行する。この時、委譲権限証明書中の委譲内容として必要なデータは（1）委譲者を識別する委譲者識別情報（委譲者名等）、（2）被委譲者を識別する被委譲者識別情報（被委譲者名等）、（3）委譲するアクセス種類（ここではj、k）、（4）委譲有効期限の4種類である。この委譲内容に対して委譲者の認証書で署名を行う。発行された委譲権限証明書52は、ネットワークまたはFD等の媒体を介して被譲渡クライアント3に渡される。

（Step 1-2）被譲渡クライアント3は、委譲権限証明書格納機能32により、受け取った委譲権限証明書52を格納する。

【0028】次に、委譲権限証明書を使って、被譲渡クライアント3が管理対象リソース13をアクセスする場合の処理ステップは次のようになる。

（Step 1-3）被譲渡クライアント3では、デジタル代理署名生成機能（アクセス要求生成部）31により、委譲権限証明書52とリソースへの処理要求（アクセス要求内容）から代理署名内容を生成し、代理署名内容に被譲渡クライアント3が署名した署名データと代理署名内容からデジタル代理署名53（アクセス要求）を生成する。生成されたデジタル代理署名53はリソース管理サーバ1に受け渡される。なお、デジタル代理署名53の例を図3に示す。デジタル代理署名53中には、委譲権限証明書52、管理対象リソースに対する処理要求を代理署名内容として含み、また代理署名内容に対する被譲渡者による署名もあわせて記載される。

【0029】（Step 1-4）リソース管理サーバ1のデジタル代理署名検証機能12では、受け取ったデジタル代理署名53について（1）被譲渡クライアントの署名の正しさと（2）譲渡クライアントの発行した委譲権限証明書52中の委譲者による署名の正しさを検証する。検証に成功した場合、デジタル代理署名検証機能12は委譲権限検証機能11にデジタル代理署名53を受け渡す。

【0030】（Step 1-5）検証に成功した場合、委譲権限検証機能（アクセス要求検証部）11では、デジタル代理署名53中から処理要求と委譲権限証明書の委譲内容を抽出し、リソース管理サーバが別途保持するアクセスコントロールリストとマッチングをとることによって被譲渡クライアント3が正しくアクセスしているかどうかを検証する。

（Step 1-6）検証に成功した場合のみ、リソースにアクセスを行う。

【0031】以上のように、委譲者が発行する委譲権限証明書の検証により、被委譲者のリソースアクセスが可能になるため、アクセス権限の一部についての権限委譲（期間限定、アクセス権限の種類の限定）に臨機応変に対応することが可能になる。また、委譲者がアクセス権限の一部の譲渡を証明する委譲権限証明書を発行できるので、一旦委譲された権限の不正利用を防ぐことができる。

【0032】実施の形態2. 以上の実施の形態1では、委譲者が一時的又は限定的な権限委譲を可能にするようにしたものであるが、次に、被委譲者が委譲者に対して、権限委譲を依頼する実施の形態を示す。図4は、このような場合のシステムのブロック構成図である。図において、リソース管理サーバ1は実施の形態1と同様の役割を持つ。

【0033】次に被譲渡クライアント3からの要求により、譲渡クライアント2から被譲渡クライアント3に、管理対象リソース13へのアクセス権限を委譲する際の動作について説明する。まず、委譲権限証明書発行の処理ステップは次のようになる。

【0034】(Step 2-1) 被譲渡クライアント3は委譲権限証明書発行申請機能34により、譲渡クライアント2に対して委譲権限証明書発行申請56(アクセス権限譲渡証明発行要求)を発行する。図8に示すように、この時、委譲権限証明書発行申請中の申請内容として必要なデータは、(1)委譲者を識別する委譲者識別情報(委譲者名等)、(2)被委譲者を識別する被委譲者識別情報(被委譲者名等)、(3)委譲するアクセス種類(ここではj、k)、(4)委譲有効期限の4種類である。この委譲内容に対して被委譲者の認証書で署名を行う。発行された委譲権限証明書発行申請56は、ネットワークまたはFD等の媒体を介して譲渡クライアント2に渡される。

(Step 2-2) 譲渡クライアント2は、委譲権限証明書発行申請検証機能(アクセス権限譲渡証明発行要求受付部)22により、受け取った委譲権限証明書発行申請56について申請内容の署名の正しさを検証し、さらにオペレータ等によって申請内容が適切かどうかを判断する。検証に成功した場合、委譲権限証明書発行申請検証機能22は委譲権限証明書発行機能21に委譲権限証明書発行申請56を受け渡す。委譲権限証明書発行機能21は受け取った委譲権限証明書発行申請56に基づき委譲権限証明書52を発行する。被譲渡クライアント3の委譲権限証明格納機能32は、譲渡クライアント2の委譲権限証明書発行機能21より委譲権限証明書52を受け取り、受け取った委譲権限証明書52を格納する。

【0035】委譲権限証明書の発行以降のプロセスは、実施の形態1と同様である。

【0036】以上のように、被委譲者からの申請を委譲者が判断することによって委譲権限証明書の発行が可能になるため、委譲者からの一方的な委譲ではなく、委譲者/被委譲者双方の委譲要求が実現でき、より柔軟な権限委譲を実現できる。

【0037】実施の形態3. 以上の実施の形態1では、委譲者が一時的又は限定的な権限委譲を可能にするようにしたものであるが、次に、委譲された権限が適切に利用されたかどうかを記録する実施の形態を示す。図5は、このような場合のシステムのブロック構成図である。図において、リソース管理サーバ1、譲渡クライアント2、被譲渡クライアント3は実施の形態1と同様の役割を持つ。4は委譲権限証明書の管理と、委譲権限行使を監査する監査ログを作成する委譲権限サーバである。すなわち、委譲権限サーバ4は、監査ログ記録装置として機能する。

【0038】次に譲渡クライアント2から被譲渡クライアント3に、管理対象リソース13へのアクセス権限を委譲する際の動作について説明する。まず、委譲権限証明書発行の処理ステップは次のようになる。

(Step 3-1) 実施の形態1と同様に譲渡クライ

アント2により発行された委譲権限証明書52は、ネットワークまたはFD等の媒体を介して権限委譲サーバ4に渡される。

(Step 3-2) 権限委譲サーバ4は、委譲権限証明書管理機能41により、受け取った委譲権限証明書52を格納する。

(Step 3-3) 権限委譲サーバ4は、委譲権限証明書配布機能42により、委譲権限証明書52を被譲渡クライアント3へ配布する。委譲権限証明書を使って、被譲渡クライアント3が管理対象リソース13にアクセスする場合の処理ステップは、実施の形態1に記載した(Step 1-3)~(Step 1-5)と同様である。

(Step 3-4) 検証に成功した場合のみ、リソースにアクセスを行う。実施の形態1において示したStep 1-5の検証結果を、権限委譲サーバ4に通知する。

(Step 3-5) 権限委譲サーバ4の監査ログ管理機能43では、Step 3-4において通知された検証結果を監査ログに記述する。権限委譲サーバでは、監査ログによって被譲渡クライアントによるアクセス履歴をチェックできる。

【0039】監査ログの例を図6に示す。監査ログは、複数の監査ログレコードと、全監査ログレコードに対する委譲権限サーバによる署名で構成される。監査ログレコードには、委譲権限サーバが発行したデジタル代理署名と、被委譲者によって実際に要求された処理、及びその検証結果が記述される。

【0040】以上のように、委譲権限証明書を権限委譲サーバで一括管理することにより、各委譲クライアントでの委譲権限証明書管理が不要になる。また、委譲した権限の使用状況が、権限委譲サーバに通知されるため、不正なリソース使用の摘発が可能となる。

【0041】実施の形態4. 実施の形態1、3では、委譲クライアントが委譲権限証明書52を発行したものであるが、次に、権限の委譲の適正性を権限委譲サーバ4で認可し、適正性が認められた後に委譲権限証明書52を含む権限委譲認可証58を被譲渡クライアント3に配布する実施の形態を示す。即ち、本実施の形態においては、権限委譲サーバ4は、アクセス権限譲渡証明認証装置として機能する。図7は、このような場合のシステムのブロック構成図である。

【0042】次に権限委譲サーバ4の認可を得て、譲渡クライアント2から被譲渡クライアント3に、管理対象リソース13へのアクセス権限を委譲する際の動作について説明する。まず、権限委譲認可証発行の処理ステップは次のようになる。

(Step 4-1) 譲渡クライアント2は権限委譲認可証発行要求機能23により、権限委譲サーバ4に対して権限委譲認可証発行要求57を発行する。図9に示す



ように、この時、権限委譲認可証発行要求57に必要なデータは(1)委譲権限証明書、(2)認可者を識別する認可者識別情報(権限委譲サーバ名等)、(3)委譲者による署名の3種類である。発行された権限委譲認可証発行要求57は、ネットワークまたはFD等の媒体を介して権限委譲サーバ4に渡される。

(Step 4-2) 権限委譲サーバ4は、権限委譲認可証発行機能46により、受け取った権限委譲認可証発行要求57の譲渡クライアントによる署名を検証する。

(Step 4-3) 署名が正しければ、同機能により権限委譲認可証58を発行する。発行された権限委譲認可証58は、権限委譲認可証管理機能47により格納される。なお、図10に権限委譲認可証58の例を示す。

(Step 4-4) 権限委譲認可証配布機能48により、権限委譲認可証58を被譲渡クライアント3へ配布する。

(Step 4-5) 被譲渡クライアント3は、権限委譲認可証格納機能35により、権限委譲認可証58を格納する。権限委譲認可証58を使って、被譲渡クライアント3が管理対象リソース13をアクセスする場合の処理ステップは、次のようになる。

(Step 4-6) 権限委譲認可証58とリソースへの処理要求から、委譲内容を生成し、委譲内容に被譲渡クライアントが署名した署名データと委譲内容からデジタル代理署名59を生成する。生成されたデジタル代理署名59はリソース管理サーバ1に受け渡される。なお、図11にデジタル代理署名59の例を示す。

(Step 4-7) リソース管理サーバ1のデジタル代理署名検証機能12では、受け取ったデジタル代理署名59について(1)被譲渡クライアントの署名の正しさを検証する。検証に成功した場合、デジタル代理署名検証機能12は権限委譲認可証検証機能14にデジタル代理署名59を受け渡す。

(Step 4-8) 権限委譲認可証検証機能14では、デジタル代理署名59から権限委譲認可証58を抽出し、検証を行う。検証に成功した場合、権限委譲認可証検証機能14はデジタル代理署名59を委譲権限検証機能11に受け渡す。

(Step 4-9) 委譲権限検証機能11では、デジタル代理署名59中から処理要求と委譲権限証明書52の委譲内容を抽出し、リソース管理サーバが別途保持するアクセスコントロールリストとマッチングをとることにより被譲渡クライアント3が正しくアクセスしているかどうかを検証する。

(Step 4-10) 検証に成功した場合のみ、リソースにアクセスを行う。Step 4-9の検証結果を、権限委譲サーバ4に通知する。

(Step 4-11) 権限委譲サーバ4の監査ログ管理機能43では、Step 4-10においてリソース管理サーバ1から通知された検証結果を監査ログに記述

する。

【0043】 以上のように、委譲権限証明書に対する認可を権限委譲サーバが行うことにより、権限の委譲時におけるなりすましを防止することができる。

【0044】 実施の形態5. 実施の形態3、4では、権限委譲サーバが委譲権限行使状態を管理していたものであるが、次に、リソース管理サーバが委譲権限行使状態を管理する実施の形態を示す。図12は、このような場合のシステムのブロック構成図である。図において、譲渡クライアント2、被譲渡クライアント3は実施の形態4と同様の役割を持つ。リソース管理サーバ1は、実施の形態4の機能に加え、譲渡クライアント2からの権限委譲認可証発行要求57を処理する権限委譲認可証発行機能17(権限委譲サーバの46に相当)、権限委譲認可証管理機能15(権限委譲サーバの47に相当)、権限委譲認可証配布機能16(権限委譲サーバの48に相当)、監査ログ管理機能18(権限委譲サーバの43に相当)を備える。

【0045】 次に譲渡クライアント2の要求により、譲渡クライアント2から被譲渡クライアント3に、管理対象リソース13へのアクセス権限を委譲する際の動作は、実施の形態3で、権限委譲サーバ4で実施していた処理をリソース管理サーバ1で行ったものと同等なので、割愛する。

【0046】 以上のように、リソース管理サーバが管理対象リソースとともに委譲権限行使状態を一括管理することにより、システム中の構成マシンが削減できる。さらに、委譲した権限の使用状況がリソース管理サーバで認識できるため、監査ログの記録にタイムラグが発生する確率がより微小となり、正確なログが取得できる。

【0047】 これまで説明してきた本発明の特徴をまとめると以下ようになる。リソースへのアクセスの一時的な譲渡を実現することを目的とした、次の構成を備えるシステム。

(a) 共有リソースを管理するリソース管理サーバ

(b) リソース管理サーバが管理するリソースに対してアクセス権限を持ち、他者にそのアクセス権限を譲渡する権利を持つアクセス権限譲渡クライアント(以下、譲渡クライアント)。

(c) リソース管理サーバが管理するリソースに対してアクセス権限を持たず、譲渡クライアントからアクセス権を譲渡されることによりリソースアクセスが可能になる被アクセス権限譲渡クライアント(以下、被譲渡クライアント)。

上で述べたシステム構成要素は次の機能を備える。

(a) 譲渡クライアントが、被譲渡クライアントに一時的な譲渡を許可する委譲権限証明書を発行する、委譲権限証明書発行機能

(b) 被譲渡クライアントがリソースに対してアクセス要求をする際に送付するデジタル代理署名を作成する

ための、デジタル代理署名生成機能

(c) 被譲渡クライアントが受け取った委譲権限証明書を格納するための、委譲権限証明書格納機能

(d) リソース管理サーバが、被譲渡クライアントが発行したデジタル代理署名を検証するための、デジタル代理署名検証機能

(e) リソース管理サーバが、被譲渡クライアントがリソースアクセスする際の権限が適切かどうかを検証する委譲権限検証機能

【0048】更に、以下の構成を追加したシステム。

(a) アクセス権限が譲渡された際の、リソースアクセス状況を管理する権限委譲サーバ。

権限委譲サーバは次の機能を備える。

(a) 権限委譲サーバが権限委譲状況を管理するために委譲権限証明書を管理する委譲権限証明書管理機能

(b) 権限委譲サーバが委譲権限証明書を譲渡クライアントから被譲渡クライアントに配布するための委譲権限証明書配布機能

(c) 権限委譲サーバが委譲されたリソースへのアクセス権限の実行状況を取得するための監査ログ管理機能

【0049】更に、以下の機能を備えるシステム。権限委譲サーバによって、権限委譲の認可を行う。

(a) 譲渡クライアントが、権限委譲サーバに対して、権限委譲認可証の発行を要求するための権限委譲認可証発行要求機能

(b) 権限委譲サーバが、譲渡クライアントからの権限委譲認可証の発行要求に対応して、権限委譲認可証を発行するための権限委譲認可証発行機能

(c) 権限委譲サーバが、権限委譲認可証を管理、配布する権限委譲認可証管理機能、及び権限委譲認可証配布機能

(d) 権限委譲サーバが委譲されたリソースへのアクセス権限の実行状況を取得するための監査ログ管理機能

(e) 被譲渡クライアントが、権限委譲サーバから発行された権限委譲認可証を格納するための権限委譲認可証格納機能

(f) リソース管理サーバが、被譲渡クライアントが発行したデジタル代理署名中の権限委譲認可証を検証するための権限委譲認可証検証機能

【0050】更に、以下の機能を備えるシステム。

(a) 被譲渡クライアントが、譲渡クライアントに対して、委譲権限証明書の発行を要求するための委譲権限証明書発行申請機能

(b) 譲渡クライアントが、被譲渡クライアントからの委譲権限証明書発行申請を検証するための委譲権限証明書発行申請検証機能

【0051】更に、以下の機能を備えるシステム。

(a) 譲渡クライアントが、権限委譲サーバに対して、権限委譲認可証の発行を要求するための権限委譲認可証発行要求機能

(b) 被譲渡クライアントが、権限委譲サーバから発行された権限委譲認可証を格納するための権限委譲認可証格納機能

(c) リソース管理サーバが、譲渡クライアントからの権限委譲認可証の発行要求に対応して、権限委譲認可証を発行するための権限委譲認可証発行機能

(d) リソース管理サーバが、権限委譲認可証を管理、配布する権限委譲認可証管理機能、及び権限委譲認可証配布機能

(e) リソース管理サーバが、被譲渡クライアントが発行したデジタル代理署名中の権限委譲認可証を検証するための権限委譲認可証検証機能

(f) リソース管理サーバが、委譲されたリソースへのアクセス権限の実行状況を取得するための監査ログ管理機能

【0052】

【発明の効果】本発明によれば、委譲者が発行する委譲権限証明書の検証により、被委譲者のリソースアクセスが可能になるため、アクセス権限の一部についての権限委譲（期間限定、アクセス権限の種類の限定）に臨機応変に対応することが可能になる。また、委譲者がアクセス権限の一部の譲渡を証明する委譲権限証明書を発行できるので、一旦委譲された権限の不正利用を防ぐことができる。

【0053】また、本発明によれば、被委譲者からの申請を委譲者が判断することによって委譲権限証明書の発行が可能になるため、委譲者からの一方的な委譲ではなく、委譲者／被委譲者双方の委譲要求が実現でき、より柔軟な権限委譲を実現できる。

【0054】また、本発明によれば、委譲権限証明書を権限委譲サーバで一括管理することにより、各委譲クライアントでの委譲権限証明書管理が不要になる。また、委譲した権限の使用状況が、権限委譲サーバに通知されるため、不正なリソース使用の摘発が可能となる。

【0055】更に、本発明によれば、委譲権限証明書に対する認可を権限委譲サーバが行うことにより、権限の委譲時におけるなりすましを防止することができる。

【0056】また、本発明によれば、リソース管理サーバが管理対象リソースとともに委譲権限行使状態を一括管理することにより、システム中の構成マシンが削減できる。さらに、委譲した権限の使用状況がリソース管理サーバで認識できるため、監査ログの記録にタイムラグが発生する確率がより微小となり、正確なログが取得できる。

【図面の簡単な説明】

【図1】 実施の形態1に係る共有リソース管理システムの構成を示す図。

【図2】 委譲権限証明書の内容を示す図。

【図3】 デジタル代理署名の内容を示す図。

【図4】 実施の形態2に係る共有リソース管理システ

1 リソース管理サーバ、2 譲渡クライアント、3  
被譲渡クライアント、4 権限委譲サーバ、11 委譲\*

54

監査ログ

監査ログレコード1

デジタル代理署名

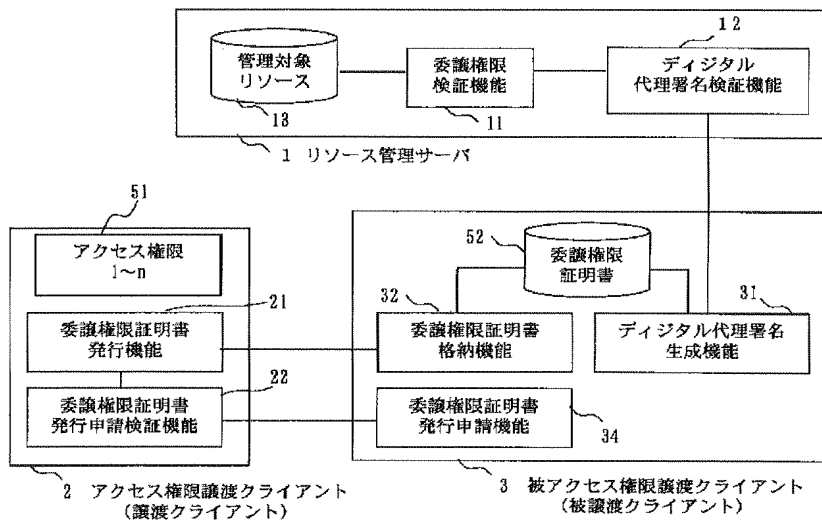
実処理要求

検証結果

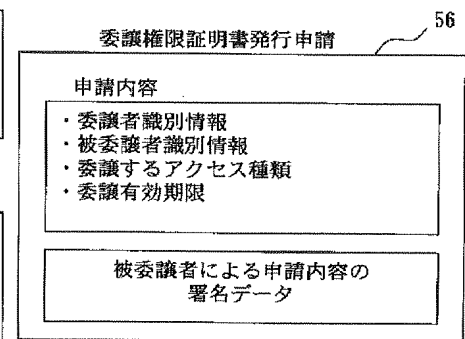
監査ログレコード2

全監査ログレコードに対する委託  
権限サーバによる署名

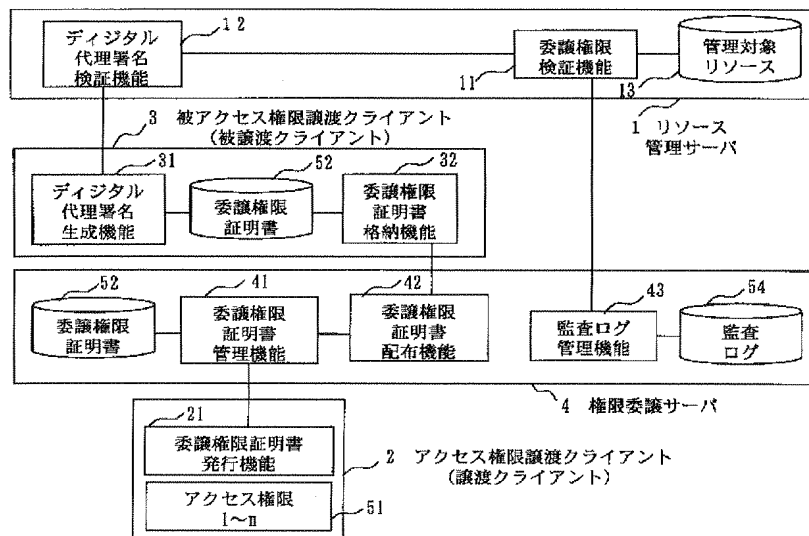
【図4】



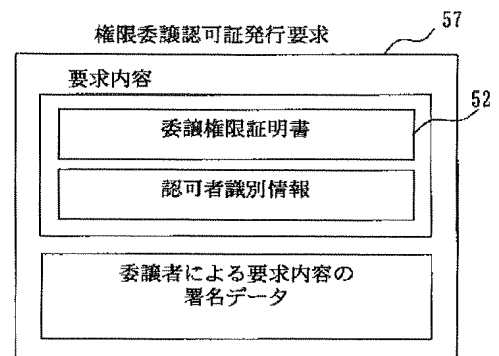
【図8】



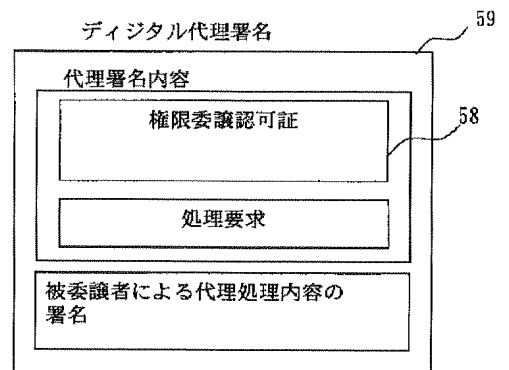
【図5】



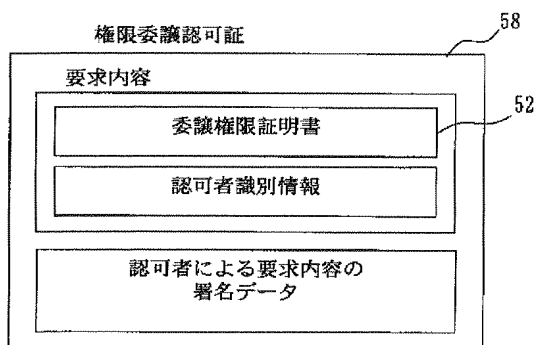
【図9】



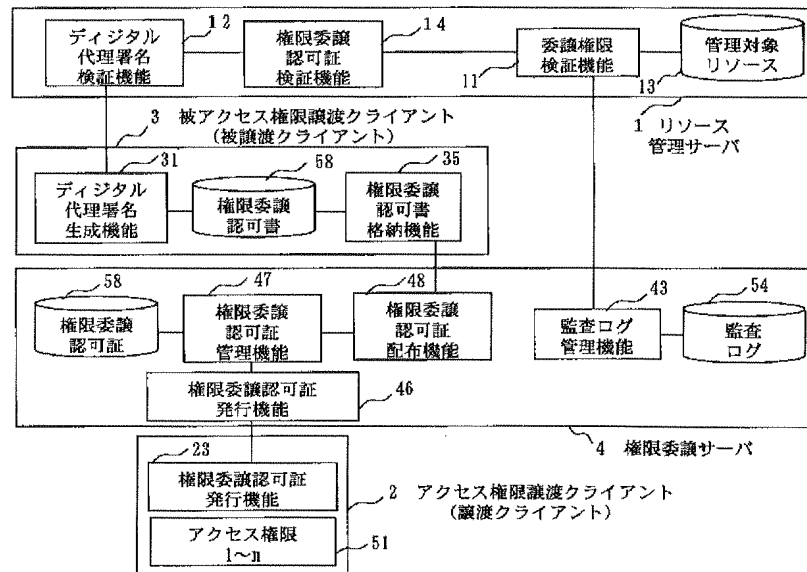
【図11】



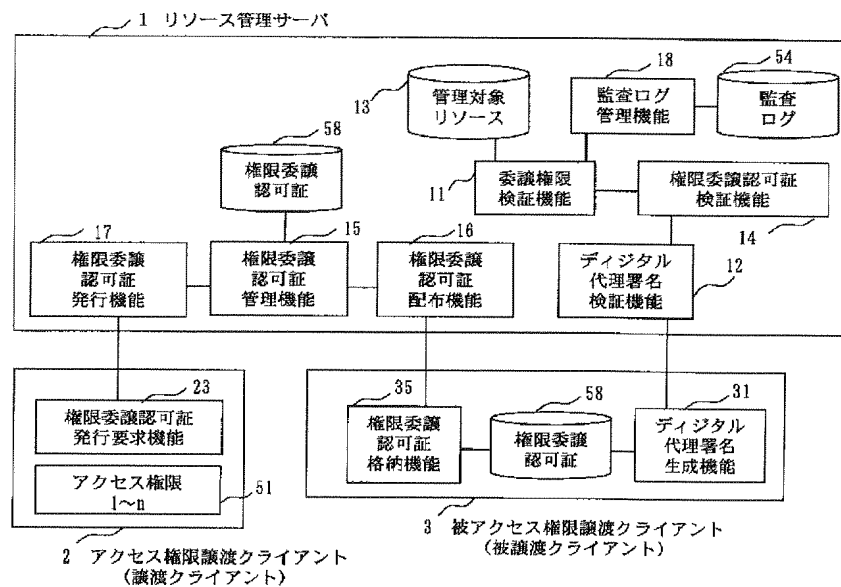
【図10】



【図7】



【図12】



【図13】

